

**Performance Audit:
Atlanta Police Department
Body-Worn Cameras**

December 2018

**City Auditor's Office
City of Atlanta**

File #18.06



CITY OF ATLANTA

City Auditor's Office
Amanda Noble, City Auditor
404.330.6750

December 2018

Why We Did This Audit

We undertook this audit because body-worn cameras enhance the transparency and accountability of interactions between citizens and the police. The chief of police requested we conduct a performance audit to assess compliance with the department's body-worn camera policy and recommend metrics for monitoring program compliance.

What We Recommended

To ensure compliance with the department's body-worn camera policies and best practices, we recommend that the chief of police:

- clarify the policy regarding recording all incidents
- update policy to remove requirement that supervisors upload use-of-force incidents and to require supervisors review audit trails to ensure involved officer has not accessed the video
- clarify criteria for categorizing videos in the policy
- establish a formal process for zone supervisors' reviews
- conduct monthly reviews of user roles and permissions
- enforce policies requiring the compliance team to review deleted footage prior to deletion
- develop standard justifications for access to videos

To ensure accountability and transparency, we recommend the chief of police monitor and track the following performance metrics :

- videos captured compared to dispatched calls
- videos uploaded within one day
- uncategorized videos
- videos streamed by supervisors
- videos deleted before the retention schedule
- videos audited by the compliance team
- audited videos that complied with activation procedures
- audited videos that complied with deactivation procedures
- audited videos that were accurately categorized

For more information regarding this report, please use the "contact" link on our website at www.atlaudit.org

Performance Audit:

APD Body-Worn Cameras

What We Found

The Atlanta Police Department's officers risk the potential loss of evidentiary data and public trust by failing to consistently use body-worn cameras to record interactions with the public. Officers assigned body-worn cameras captured video for 33% of officer-dispatched calls from November 2017 to May 2018.

Officers also delayed activation and prematurely deactivated the body-worn cameras for many incidents. In our random sample of 150 videos, 61% were activated and 47% were deactivated according to policy. Overall, we estimated that 30%-46% of videos complied with both activation and deactivation procedures.

Officers uploaded 74% of videos according to the department's procedures within one day of the date they were recorded. Officers also categorized almost all videos but could improve accuracy of categories assigned. In our sample, officers miscategorized 22 videos, including one that the department agreed should have been categorized as a use of force incident. Miscategorized videos may be deleted prematurely, which may not comply with state law.

Supervisors are responsible for ensuring that officers comply with camera policies; however, supervisors reviewed only 2% of all videos uploaded between November 2016 and May 2018. Departmental procedures do not specify a formal process regarding the number of videos to review or include criteria to ensure compliance with recording policies.

Compliance staff are not reviewing videos as required to monitor compliance with camera policies and ensure video footage is not prematurely deleted. The team reviewed less than 1% of videos prior to deletion between November 2016 and May 2018. We also identified 64 videos that were deleted by users who should not have been authorized to delete videos from the system.

Management Responses to Audit Recommendations

Summary of Management Responses		
Recommendation #1:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police clarify the policy to state whether all officers responding to an incident must record body camera video.	
Response & Proposed Action:	The existing SOP does not provide the level of clarity required for a large organization. The SOP will be modified to eliminate those factors causing confusion.	Agree
Timeframe:	December 2018	
Recommendation #2:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police update the policy to remove the requirement that supervisors upload videos of use-of-force incidents and to require supervisors to review the audit trail to ensure the involved officer has not accessed the video prior to writing the report.	
Response & Proposed Action:	Due to a more complete audit trail, the policy will be revised to remove the requirement that supervisors upload videos of use-of-force incidents. The policy will now require the immediate supervisor to review the audit trail for compliance by the involved officer with the policy not to access the video prior to completing the initial incident report.	Agree
Timeframe:	December 2018	
Recommendation #3:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police clarify criteria for labeling and categorizing videos in standard operating procedures.	
Response & Proposed Action:	The SOP has too many coding options, which has caused confusion and diminished performance. Initially there were 32 coding options, this has been reduced to 19, and the goal is 10 options. This reduction of choices should provide the necessary adjustments to allow for greater efficiency and consistency.	Agree
Timeframe:	December 2018	
Recommendation #4:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police establish a formal process for zone supervisors' periodic reviews, including the number and selection of videos, frequency, and required documentation.	
Response & Proposed Action:	Each Zone is going to be required to have their administrative sergeant audit 25 recordings every 2-weeks. They will be required to document the specific recordings examined, whether they were properly labeled, whether the officer met stated recording requirements, and whether the Zone's UAF footage corresponds to the number of UAF incidents captured in the 911 Center. The Audit Team will be responsible for managing compliance with this requirement.	Agree
Timeframe:	January 2019	

Recommendation #5:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police conduct monthly reviews of user roles and permissions to determine if non-administrator users can delete videos.	
Response & Proposed Action:	The department recognizes the need to regularly update access controls in the Evidence.com platform. There are personnel that depart, and others who change roles within our agency. Those that depart must be removed from Evidence.com access, and those who change roles need to have access appropriate to their assigned position. Tracking access also allows the BWC Team to track the status of BWCs no longer assigned and enables the team to put them back into circulation. The updating of access controls within Evidence.com will occur regularly, at least monthly.	Agree
Timeframe:	December 2019	
Recommendation #6:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police enforce policies requiring the compliance team to review all deleted footage prior to deletion for miscategorization.	
Response & Proposed Action:	The retention period was modified, and all videos are saved for 5-years. Additionally, there are only 2 individuals with the authority to delete videos, and their accounts will be cross-checked by supervisory personnel. This policy amendment was made during the audit.	Partially Agree
Timeframe:	Complete	
Recommendation #7:	To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police develop standard justifications for accessed footage to ensure compliance with the policy.	
Response & Proposed Action:	<p>The requirement to provide a specific reason for viewing a video is not an essential metric. The "notes box" is only available in Evidence.com after the video is uploaded, you are unable to add notes as to why you viewed a video in the Axon View App or in Axon Sync on the MDT, so it is not trackable across the range of viewing options.</p> <p>We are requiring that administrative sergeants and supervisors review BWC video to ensure the BWCs are activated and deactivated in accordance with policy, and not interrupted during recording. The supervisors will also audit to ensure the BWC is used according to policy. Only the officer assigned the BWC, his immediate supervisor(s), and the administrative sergeant can access the individual officer's BWC in Evidence.com. The requirement to label why a video is accessed only in Evidence.com, and not in the other viewing options makes this metric impossible to accurately track and enforce. The SOP will be amended accordingly.</p>	Agree
Timeframe:	January 2019	

- Recommendations #8–16:** To ensure accountability and transparency, we recommend the chief of police monitor and track the following performance metrics for the number and percentage of:
8. videos captured compared to the number of dispatched calls, using the 80% threshold as a comparative benchmark
 9. videos uploaded to the system within one day
 10. uncategorized videos
 11. videos streamed by supervisors
 12. videos deleted before the retention schedule
 13. videos audited by the compliance team
 14. audited videos that complied with activation procedures
 15. audited videos that complied with deactivation procedures
 16. audited videos categorized accurately

Response & Proposed Action: Metrics must be developed that allow for improved performance. The Zone audits will encompass much of the above-referenced, while a final audit checklist is still being identified. **Agree**

Timeframe: January 2019



CITY OF ATLANTA

AMANDA NOBLE
City Auditor
anoble@atlantaga.gov

STEPHANIE JACKSON
Deputy City Auditor
sjackson@atlantaga.gov

CITY AUDITOR'S OFFICE
68 MITCHELL STREET SW, SUITE 12100
ATLANTA, GEORGIA 30303-0312
<http://www.atlaudit.org>
(404) 330-6452
FAX: (404) 658-6077

AUDIT COMMITTEE
Marion Cameron, CPA, Chair
Daniel Ebersole
Danielle Hampton
Amanda Beck, PhD

December 3, 2018

Honorable Mayor and Members of the City Council:

We undertook this audit because body-worn cameras enhance the transparency and accountability of interactions between citizens and the police. The chief of police requested we conduct a performance audit to assess compliance with the department's body-worn camera policy and recommend metrics for monitoring program compliance.

The Audit Committee has reviewed this report and is releasing it in accordance with Article 2, Chapter 6 of the City Charter. We appreciate the courtesy and cooperation of city staff throughout the audit. The team for this project was Rebecca Robinson, Ivy Williams, and Diana Coomes-Lynn.

Amanda Noble
City Auditor

Marion Cameron
Chair, Audit Committee

Atlanta Police Department Body-Worn Cameras

Table of Contents

Introduction.....	1
Background.....	1
Almost Half of Sworn Officers Are Assigned Body-worn Cameras.....	2
All Six Police Zones and Some Special Programs Use Body-Worn Cameras.....	5
Implementation and Compliance Are Shared Responsibilities	6
Audit Objectives.....	7
Scope and Methodology	7
Findings and Analysis	9
Clearer Guidance and Performance Monitoring Could Strengthen Compliance with Camera Policy.....	9
Officers Are Not Using Body-Worn Cameras As Intended	10
Officers Uploaded and Categorized Almost All Videos Captured	14
It is Unclear How Supervisors Assess Compliance with Camera Policies.....	18
Users Failed to Document Video Access.....	19
Video Management System Deleted Videos According to Policy, But Manual Deletions Bypassed System Controls	21
Compliance Administrators Could Improve Training and Monitoring Efforts	23
Recommendations	25
Appendix	27
Appendix A: Management Review and Response to Audit Recommendations	29

List of Exhibits

Exhibit 1: Almost Half of Sworn Officers Are Assigned Body-Worn Cameras.....	2
Exhibit 2: Body-worn Camera Captures Officer's Field of Vision	3
Exhibit 3: Body-Worn Camera Program Was Implemented in Stages	5
Exhibit 4: Officers Have Created Nearly 500,000 Recordings Since the Program Began	6
Exhibit 5: Most E911 Dispatched Calls Had No Body-Camera Footage.....	12
Exhibit 6: Officers Failed to Activate and Deactivate Cameras According to Policy	13
Exhibit 7: Most Body-Worn Camera Videos Were Uploaded Within One Day of Creation ..	15
Exhibit 8: Cyberattack May Have Affected Video Categorization	17
Exhibit 9: Users Did Not Explain Reasons for Accessing Video Footage	20
Exhibit 10: Videos Were Retained According to Retention Schedule	22
Exhibit 11: Administrators Do Not Review Camera Footage According to Policy	24

Introduction

We undertook this audit because body-worn cameras enhance the transparency and accountability of interactions between citizens and the police. The Atlanta Police Department began deploying body-worn cameras in 2016, beginning with Zone 4 in Southwest Atlanta and rolling them out to the other patrol zones throughout 2017. The chief of police requested we conduct a performance audit to assess compliance with the department's body-worn camera policy and recommend metrics for monitoring program compliance.

Background

Body-worn cameras are relatively small devices (slightly larger than a deck of playing cards) that record interactions between community members and law enforcement officers. The video recordings can be used to promote transparency, increase accountability, and discourage inappropriate behaviors by both officers and the public.

The Atlanta City Council passed Resolution No. 14-R-4007 in 2014, requesting the chief of police conduct research and make recommendations on the feasibility of using wearable video cameras. Shortly after the resolution passed, the Atlanta Citizen Review Board (ACRB), which provides oversight of misconduct accusations against sworn members of the city's police and corrections departments, released a report which stated that although the cameras could be a valuable accountability tool, "(body-worn cameras) alone will not yield the anticipated results unless there is strong policy, effective management and enforcement, and a general change in policing culture."¹

The Atlanta City Council approved Resolution No. 16-R-4096 in August 2016, authorizing the police department to procure 1,200 body-worn cameras and video storage from Taser International for \$5.6 million. The city entered into a cooperative purchasing agreement held by the City of San Antonio, Texas, to purchase the equipment; the contract is for a five-year term with the option for two one-year renewals. The department began deploying body-worn

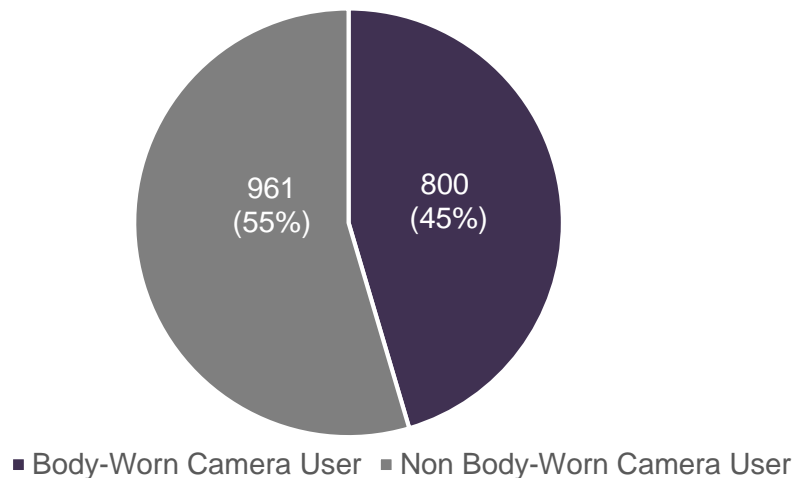
¹ *Atlanta Citizen Review Board Study on Body-worn Cameras (BWCs) and Discussion of Concerns and Recommendations on BWCs for Atlanta Police Officers, 2014*

cameras in late 2016, beginning in Zone 4 and rolling them out to the other patrol zones throughout 2017.

Almost Half of Sworn Officers Are Assigned Body-worn Cameras

As of May 2018, approximately 800 (45%) of the Atlanta Police Department's 1,761 sworn officers are assigned body-worn cameras while on duty, based on information from the program's compliance administrator. The police department's policy requires officers ranked at sergeant and below (1,648, or 94% of total sworn officers) to use the body-worn cameras during regular and extra shifts. Camera use by officers ranked at lieutenant or higher is voluntary.

Exhibit 1: Almost Half of Sworn Officers Are Assigned Body-Worn Cameras



Source: Video storage and management system (Evidence.com) report and active employee report from Oracle

Body-worn Cameras Must Be Manually Activated and Deactivated

The police department's body-worn cameras are attached to the officer's chest area of the uniform with a strong magnet. The camera placement is intended to capture activity within the officer's field of vision. The body-worn camera captures both audio and video and must be activated by pressing a button on the front of the camera device (see Exhibit 2). The officer must press the button again to stop recording. According to police department staff, camera batteries typically last ten hours on a full charge.

Exhibit 2: Body-worn Camera Captures Officer's Field of Vision



Source: Prepared by auditors with information from the Atlanta Police Department website and TASER Axon Body 2 Quick Start Guide

Officers are responsible for capturing, uploading, and categorizing video footage, as well as maintaining videos for record retention purposes:

- **Capturing video**—officers power on their devices by sliding the power switch at the top of the device. Once the camera is powered on, it stays in buffering mode until the event button is double-tapped to begin capturing video. Once activated, the camera adds two minutes of audio-less video to the beginning of the incident. The user presses and holds the event button to deactivate the camera, which returns the device to buffering mode.
- **Uploading footage**—officers can upload captured footage by either docking the device in its charger or by connecting the device to a computer or mobile device. Docking the device to the charger automatically uploads the video to a cloud-based storage and management system called Evidence.com, deletes the footage from the device, and charges the camera.

Uploading footage using a computer or mobile data terminal device (MDT) gives officers access to software that can stream, upload, and categorize selected videos. Officers can also pair the body-worn camera with a smart phone to

stream, categorize, and label videos; this option does not have uploading capabilities.

- **Categorizing videos**—once uploaded, officers are responsible for adding a category tag to each video based upon what events occur during the footage, for example, as a traffic accident or arrest.
- **Retaining records**—after a video is categorized, the video management system assigns an automatic deletion date according to the department's retention schedule, consistent with the requirements of the Georgia Open Records Act, which requires videos from law enforcement body-worn devices to be retained for at least 180 days from the date of recording. Videos that are part of a criminal investigation, that show a vehicular accident, that show the detainment or arrest of an individual, or that show a law enforcement officer's use of force are required to be retained for 30 months. As of June 2018, the department's retention policy was updated to retain all video data for at least five years; homicide-related video is maintained indefinitely.

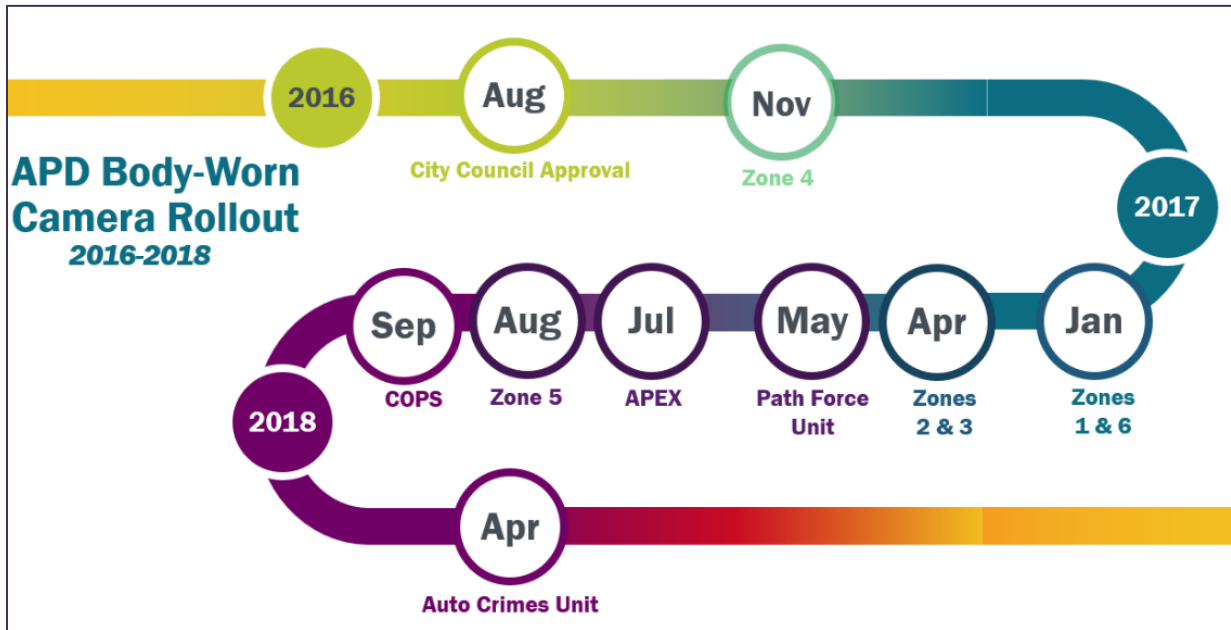
Departmental policy requires officers to place the camera in event (recording) mode “upon arriving on scene of all calls for service requiring recording of an incident, or when interacting with the public in a law enforcement capacity which the officer and/or his or her supervisor deems necessary to record and document.” Officers are required to upload all video footage before the end of their shift. Each video must be tagged with a category and given a case number for identification purposes.

Body-worn cameras are assigned to officers individually, and each camera is linked to the officer's unique identification number. Officers have access only to video they upload into Evidence.com, the video management system. The system maintains an audit trail of users who access video data to protect the integrity and privacy of the recorded data and preserve the chain of custody. Supervisors and administrators may access all data and user information associated with that evidence, except restricted videos. One assigned user role, the system super administrator, has full access and privileges to all evidence and footage uploaded.

All Six Police Zones and Some Special Programs Use Body-Worn Cameras

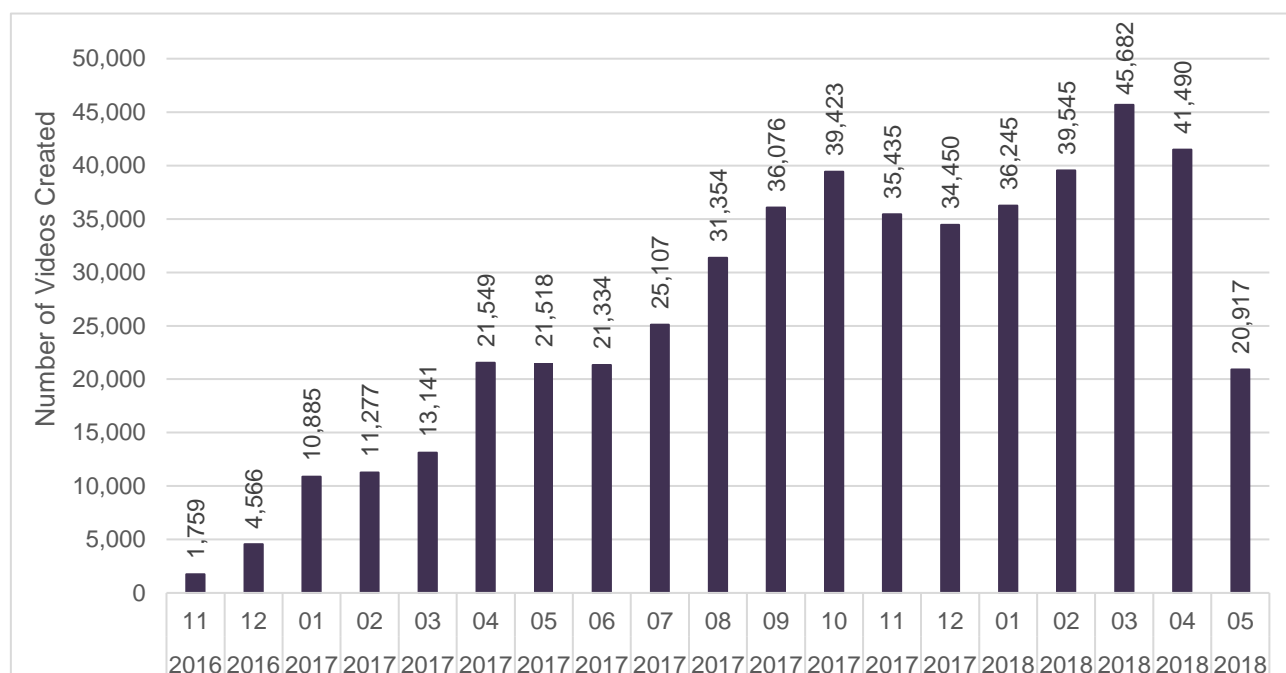
Once the police department began implementing body-worn cameras in Zone 4, it continued the rollout in other zones and programs as well (see Exhibit 3). As of April 2018, Zones 1 through 6 use the cameras, along with special police programs such as the Path Force Unit, APEX (Atlanta Proactive Enforcement and Interdiction) Unit, COPS (Community Oriented Policing Section), and Auto Crimes Unit.

Exhibit 3: Body-Worn Camera Program Was Implemented in Stages



Source: Developed by auditors with information from the Atlanta Police Department

Body-worn camera users created and uploaded 491,753 videos from November 21, 2016, to May 15, 2018, as shown in Exhibit 4. The number of video recordings have increased as the program expanded.

Exhibit 4: Officers Have Created Nearly 500,000 Recordings Since the Program Began

Source: Evidence.com, November 16, 2016 through May 15, 2018

The top six categories for videos uploaded from November 2016 through May 2018 were:

- miscellaneous & non-enforcement (conducted police business, but did not have to enforce the law),
- criminal report,
- arrest,
- traffic stop,
- traffic accidents, and
- investigations & surveillance

Those categories accounted for 388,229 of the total files, or 78.9% of all video. Footage related to use of force incidents accounts for less than 1% of all videos.

Implementation and Compliance Are Shared Responsibilities

The police department has designated a compliance administrator who is responsible for providing training, keeping an accurate list of camera users, controlling the equipment inventory, and maintaining the online video footage. The compliance administrator's duties also include auditing the video footage to ensure that officers adhere to policies and procedures governing use of the cameras. The administrator has a team of five people to assist with these responsibilities.

Supervisors are responsible for ensuring employees under their command use the cameras according to policy and training. They are also responsible for retrieving, uploading, and categorizing footage from use of force events.

Audit Objectives

This report addresses the following objectives:

- Do body-worn camera users comply with the Atlanta Police Department's standard operating procedures?
- What metrics should the Atlanta Police Department consider when assessing officers' compliance with policy and best practices?

Scope and Methodology

We conducted this audit in accordance with generally accepted government auditing standards. We reviewed video footage and information related to body-worn cameras from November 2016 through June 2018.

Our audit methods included:

- interviewing subject matter experts from the Atlanta Police Department, Atlanta Citizen Review Board, and Atlanta Police Foundation about body-worn camera programs
- reviewing city code and departmental policies to understand requirements
- researching best practices for body-worn cameras and related controls
- analyzing system data for capturing videos compared with CAD (computer-aided dispatch) activity
- analyzing video upload and categorization by role to ensure compliance with policy, particularly for use of force incidents
- analyzing Evidence.com system controls to determine whether videos were retained in accordance with retention guidelines and whether videos could be deleted by unauthorized users

- observing roll call and ride-alongs with police officers from various zones to understand how body-worn cameras are used on patrol

Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Findings and Analysis

Clearer Guidance and Performance Monitoring Could Strengthen Compliance with Camera Policy

The Atlanta Police Department's officers risk the potential loss of evidentiary information and public trust by failing to consistently use body-worn cameras to record interactions with the public. Officers assigned body-worn cameras captured video for 33% of officer-dispatched calls occurring from November 2017 through May 2018. Police department staff told us they would expect 80% of all incidents to have corresponding video.

Officers also delayed activation and prematurely deactivated the body-worn cameras for many incidents. In our random sample of 150 videos, 61% were activated according to policy. Officers are required to activate the cameras when arriving on the scene for all calls for service, when interacting with the public in a law enforcement capacity, or during emergency driving with lights and sirens. Officers deactivated cameras according to policy in 47% of the sampled videos—when the call is complete, when the event is controlled, or at a supervisor's direction. Overall, we estimated that 30%-46% of videos complied with both activation and deactivation procedures. We recommend that the department monitor and track the number of videos captured to ensure officers are properly using the cameras.

Once recorded, officers uploaded most videos according to the department's procedures. Of the 491,753 videos captured between November 21, 2016, and May 15, 2018, 74% were uploaded within one day of the date they were recorded. Officers are required to upload videos by the end of their shifts. Officers also categorized almost all videos but could improve accuracy of categories assigned. In our sample, officers miscategorized 22 videos, including one that the department agreed should have been categorized as a use of force incident. The video management system determines the retention period of videos based on category type. If officers do not accurately categorize videos, they may be deleted prematurely, which may not comply with state law. We recommend that the department clarify criteria for labeling and categorizing videos in standard operating procedures and that supervisors and the compliance team check the accuracy of categories assigned as they review videos on a sample basis.

Supervisors are responsible for ensuring that officers comply with camera policies; however, supervisors reviewed only 2% of all videos uploaded between November 2016 and May 2018. Departmental procedures do not specify a formal process regarding the number of videos to review or include criteria to ensure compliance with recording policies. We recommend that the department strengthen the policy to require the supervisors to review a specific number of videos each month and the necessary criteria to ensure compliance.

Compliance staff are not reviewing videos as required to ensure that officers comply with the camera policy and to ensure that camera footage is not prematurely deleted. From November 2016 through May 2018, the administrator streamed only 1,325 of more than 490,000 videos. Beginning December 2017, the department required the compliance administrator to randomly review at least 25 body-worn camera videos on a weekly basis, which was not met. Also, the compliance team reviewed less than 1% of 155,094 videos prior to deletion. The compliance team is required to review video footage scheduled for deletion to reduce the risk of premature deletion, primarily due to incorrect categorization. The team has a seven-day window after the retention period ends to review videos before the system permanently deletes the footage. We recommend the department monitor and track the number of videos reviewed as required by the policy.

System controls generally complied with the department's body-worn camera footage retention policy—99% of videos were deleted from the video storage system according to the retention schedule. We identified 64 videos that were deleted by supervisors; department officials stated that non-administrative users should not be able to delete video evidence from the system. The department should review user configurations to determine if other users could delete videos to ensure transparency and accountability.

Officers Are Not Using Body-Worn Cameras As Intended

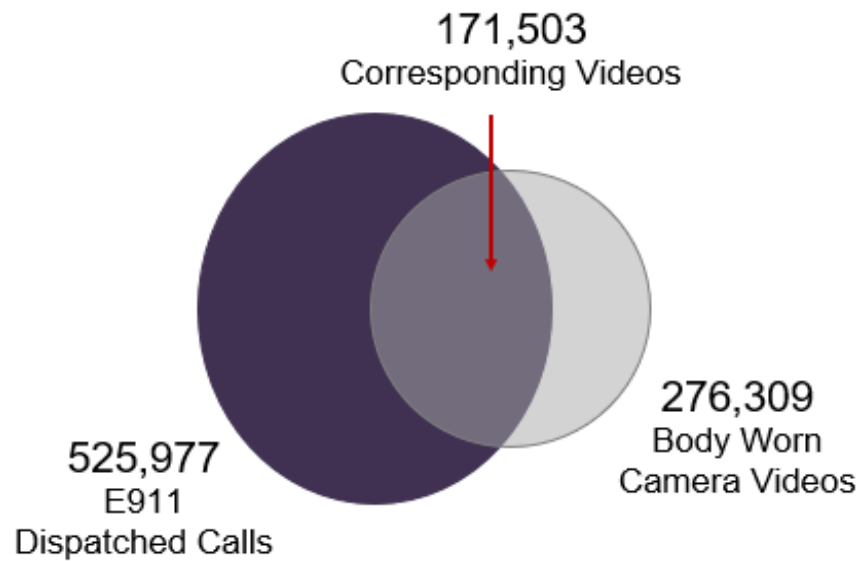
Officers failed to capture two-thirds of the dispatched calls from November 2017 through May 2018. On-duty officers receive services calls from dispatchers in the E911 communications center and also respond to self-initiated calls. According to compliance staff, about 80% of the E911 calls should have corresponding video footage. Also, of our random sample of 150 videos, we found that officers activated the body-worn cameras properly in 91 (61%) of videos; officers deactivated cameras in 71 (47%) of videos consistent with departmental procedures.

In addition, 70 of 150 videos had multiple officers on scene, but only 43 of the 70 contained recordings from all officers at the scene. Departmental procedures require all officers to record interactions with the public, but are silent on whether all officers must record when dispatched to the same incident. Failure to capture video limits the effectiveness of the body-worn camera program. We recommend the department monitor the number of videos captured and review footage to ensure officers are properly using body-worn cameras. We also recommend the department clarify in the procedures whether all officers responding to the same incident must record and upload body-worn camera video.

Most dispatched calls did not have corresponding body-worn camera footage. From November 2017 through May 2018, 67% of dispatched calls (354,474 of 525,977) had no matching body-worn camera footage in the video management system (see Exhibit 5). On-duty officers receive service calls from dispatchers in the E911 communications center and also respond to self-initiated calls. Officers who are responding to calls in these zones have been assigned body-worn cameras. According to the department's procedures, officers should record all service calls while on or off duty. Dispatchers assign each service call a case number and record the badge identification number of the responding officer. Once a dispatcher provides the case number to the responding officer, the officer documents the number and uses it to label the associated video at the end of shift.

We reviewed 525,977 dispatch records from a CAD (computer-aided dispatch) report and compared them to 276,309 videos from the video management system over the same 7-month period. Compliance staff told us that while dispatched calls without matching video could be canceled calls or calls that did not require a police action, they would expect officers to have body-worn camera videos for 80% of dispatched calls. Dispatched calls without matching videos may be calls that did not require police action, such as removing a cat from a tree or providing someone with directions.

Exhibit 5: Most E911 Dispatched Calls Had No Body-Camera Footage

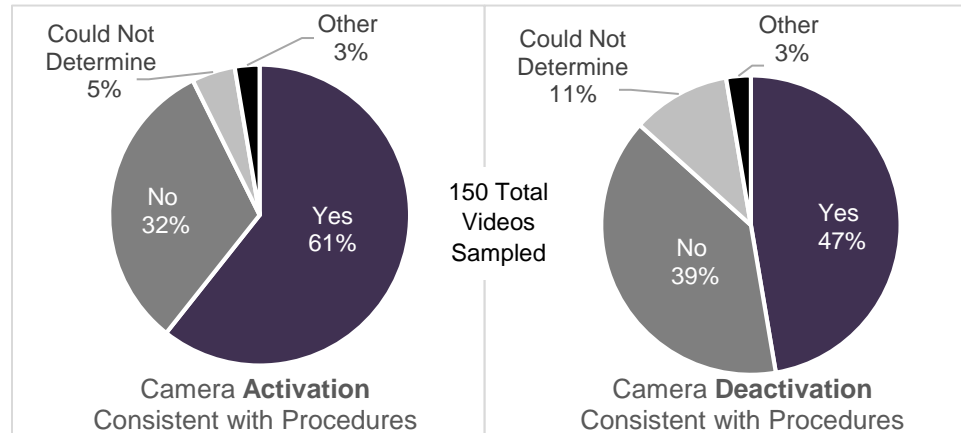


Source: Auditor's analysis of computer-aided dispatch report data and video management system data from November 2017 through May 2018

Failure to capture video limits the effectiveness of the body-worn camera program. We recommend the department monitor the dispatched calls for service and number of videos captured to ensure officers are properly using body-worn cameras.

Officers delayed activation and prematurely deactivated the body-worn cameras for many incidents and inconsistently recorded when multiple officers responded to a call. In a random sample of 150 videos, we found that officers activated cameras according to policy in 91 (61%) of the videos. Officers deactivated cameras according to policy in 71 (47%) of the videos (see Exhibit 6). Overall, we estimate at a 95% confidence level that 30%-46% of videos uploaded through May 2018 complied with both activation and deactivation procedures. In some instances, as shown in Exhibit 6, we were unable to determine whether officers activated or deactivated cameras properly.

Exhibit 6: Officers Failed to Activate and Deactivate Cameras According to Policy



Source: Auditor's analysis of sample of 150 videos in the from the video management system from November 2016 to May 2018

Some of the premature deactivations involved officers deactivating and reactivating while on the same call for service; 33 of 150 videos (22%) had multiple recordings for the same officer for the same call. We also found that 70 of 150 videos had multiple officers on scene but only 42 of those 70 (60%) had videos for all the additional officers on scene, known as “multi-cam.”

We conducted a representative statistical sample based on the number of videos that officers created in each of the six zones. We streamed each video to determine whether officers were activating their body-worn cameras in accordance with standard operating procedures. Officers are required to activate the cameras when arriving on the scene for all calls for service, when interacting with the public in a law enforcement capacity, or during emergency driving with lights and sirens. Cameras are to remain in record mode until the call is complete, when the event is controlled, or a supervisor directs the officer to deactivate.

In training sessions, the compliance team attempts to instill activation and deactivation into officers' muscle memory. When an officer does not properly activate and deactivate the body-worn camera, community relations may be adversely affected due to diminished transparency, and valuable evidence may be lost. We recommend that the department clarify and reiterate activation and deactivation requirements and incorporate those specific procedures into training sessions. We also recommend the department clarify in the procedures whether all officers responding to the same incident must record and upload body-camera video.

Officers Uploaded and Categorized Almost All Videos Captured

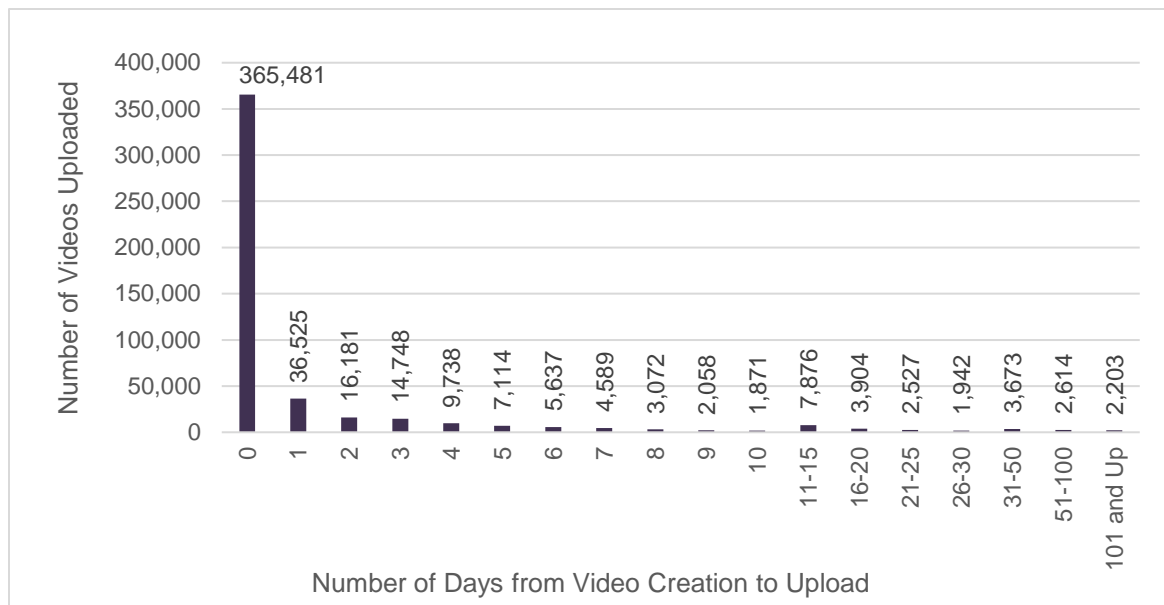
Of the 491,753 body-worn camera videos captured between November 2016 and May 2018, 74% were uploaded within one day of creation, consistent with the department procedures. The department requires users to upload video footage by the end of the shift.

Two-thirds of the use of force videos were uploaded by users with officer access; departmental procedures require videos related to use of force incidents to be uploaded by a supervisor. The video system did not make a distinction between who created and uploaded the footage when placed in the dock. We recommend that the department monitor and track video uploading to ensure compliance. We also recommend that the department update the policy to remove the requirement that supervisors upload videos of use-of-force incidents and to require supervisors to review the audit trail to ensure the involved officer has not accessed the video prior to writing the report.

The users categorized almost all (99.6%) of the videos captured. Most uncategorized videos were uploaded between March and May 2018, which was the period after the city was victim to a cyberattack. Officers told us they had limited access to functioning computers, which may have prevented them from categorizing videos promptly.

Three-quarters (74%) of videos captured between November 2016 and May 2018 were uploaded within one day of creation. We also found that 88% of videos were uploaded within 3 days and 95% were uploaded within 9 days of creation (see Exhibit 7). According to the department's policy, employees who are assigned a camera are responsible for ensuring that all video footage and data is uploaded before the end of their shift. The compliance administrator's team stated there may be delays of two-to-three days between recording and uploading body-worn camera footage if users work extra jobs after their regular shift. The policy also requires users who are assigned body-worn cameras to wear and use their devices during extra jobs, but users may not return to the precinct to upload the footage until two or three days later.

Exhibit 7: Most Body-Worn Camera Videos Were Uploaded Within One Day of Creation



Source: Data from video management system from computer-aided dispatch report data from November 2016 to May 2018

Regularly uploading videos is important because once the camera's memory is full, it will not record additional data and users may fail to record events of evidentiary significance. Also, if the camera falls or is pulled off of an officer and subsequently lost, the data stored on the camera's memory is also lost. We recommend that the department monitor and track video uploading to improve compliance.

One-fourth of all use of force videos were uploaded by supervisors, as required by the department. Less than 1% (1,480) of the 491,753 videos uploaded between November 2016 and May 2018 were categorized as use of force incidents. We were able to confirm that supervisors uploaded 404 (27%) of those videos; another 67% of the use of force videos were uploaded by users with officer access. According to standard operating procedures, any use of force incident captured by the body-worn camera must be uploaded by a supervisor before the end of the user's shift and officers are required to complete incident reports prior to viewing the related videos. This helps to promote accountability and accuracy.

The video management system makes no distinction between the owner of the footage and the uploader if a zone supervisor uses the camera dock to upload the footage; therefore, more supervisors may be uploading the use of force videos than identified by the system. The compliance administration team was unaware of this issue.

Through our interviews with supervisors, we identified inconsistencies regarding zone supervisors' understanding of their responsibility related to uploading use of force footage. One zone supervisor stated that he was responsible for uploading, while another zone supervisor stated he did not upload footage after use of force incidents.

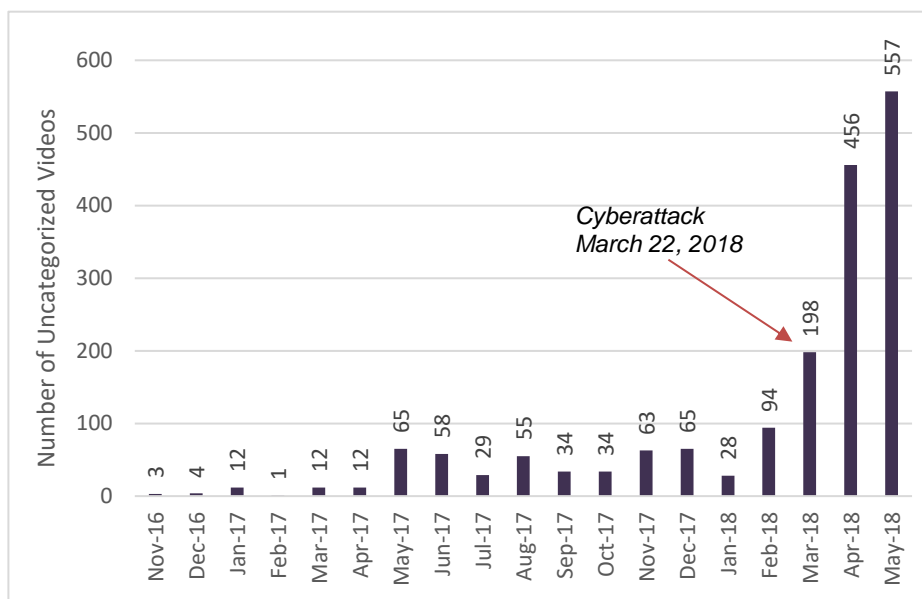
According to the department, the intent behind having the supervisor dock the involved officer's camera in a use of force incident was to establish an immediate audit trail regarding the viewing of the video. The department's policy requires the involved officer to write the initial report prior to viewing his/her video associated with a use-of-force incident. Because officers could view the video on their cellphones using the Axon View App, which did not have an audit trail, the policy required supervisors to gain custody of the camera and upload the video.

The department stated that the Axon View App is now part of the Evidence.com audit trail. "Since all video is encrypted, cannot be altered, and there is an immediate audit trail, it is no longer essential that a supervisor gain control of the BWC to upload the use-of-force video." The audit trail provides sufficient tracking to monitor compliance with the department's policy.

We recommend that the department update the policy to remove the requirement that supervisors upload videos of use-of-force incidents and to require supervisors to review the audit trail to ensure the involved officer has not accessed the video prior to writing the report.

Officers categorized 99.6% of all videos created between November 2016 and May 2018. A total of 1,780 of 491,753 (0.4%) videos were uncategorized as of May 2018 (see Exhibit 8). Two-thirds of the uncategorized videos were recorded during March through May 2018, which was the period after the cyberattack. While the attack did not directly impact the system, officers told us they had limited access to functioning computers, which may have limited their ability to categorize videos.

Exhibit 8: Cyberattack May Have Affected Video Categorization



Source: Data from video management system from computer-aided dispatch report data from November 2016 to May 2018

After uploading videos, officers are responsible for adding a category tag to each video based upon what events occur during the footage, for example, a traffic accident or arrest. The category determines the retention period of the footage. The department's policy requires users to categorize and label footage at the end of each shift.

While officers categorized most videos, some were miscategorized and some were not labeled with case numbers. Standard operating procedures require officers to label videos with case numbers, but they failed to label 10% of videos recorded between May 2017 and June 2018. Furthermore, in our sample of 150 videos, we found that officers miscategorized 22 videos, including one video that the department agreed should have been categorized as a use of force incident. Other than to require officers to add a category tag to the footage, the department's body-worn camera policy does not address categorization. Training materials list the categories and the logistics of accessing videos to categorize them, but it is unclear whether instructors train officers in what categories are appropriate to use in a given situation.

The video management system assigns an automatic deletion date for videos based on the category. The retention dates are set up to comply with the requirements of the Georgia Open Records Act. The department's retention policy was recently updated to retain all video data for at least five years; homicide related video is

maintained indefinitely. If officers do not properly categorize videos, they may be deleted by the system prematurely, which may not comply with state law. Also, if officers fail to label videos with case numbers, the footage may be overlooked as evidence in court proceedings.

We recommend that the department clarify criteria for labeling and categorizing videos in standard operating procedures.

It is Unclear How Supervisors Assess Compliance with Camera Policies

Supervisors are responsible for ensuring that officers comply with camera policies, but we found that supervisors streamed only 2% of all videos for review between November 2016 and May 2018. Also, departmental procedures do not specify a formal process for reviewing officers' footage to assess compliance with the body-worn camera policies. To enhance accountability, we recommend the department strengthen the policy to require the supervisor to review a specific number of videos each month and the necessary criteria to ensure compliance.

Supervisors streamed 8,372 (2%) of the 491,753 videos created from November 2016 through May 2018. Only one of 148 supervisors streamed body-worn camera footage monthly. Some zone supervisors told us they did not have a process for reviewing videos. Some supervisors did not review footage at all. According to departmental procedures, supervisors are responsible for ensuring officers' compliance with body-worn camera policies, but do not explain how the supervisors should ensure compliance. The department may miss out on opportunities to improve training and identify departmental weaknesses if zone supervisors fail to regularly review videos.

Best practices recommend that zone supervisors conduct periodic reviews of body-worn camera footage to ensure compliance with standard operating procedures and to identify videos for training and instructional purposes. The Georgia Association of Chiefs of Police and the International Association of Chiefs of Police recommend random monthly reviews of officers' footage. The Police Executive Research Forum (PERF) suggests that zone supervisors monitor officers who are on probation and those who the department has identified to participate in early intervention for exhibiting patterns of misconduct.

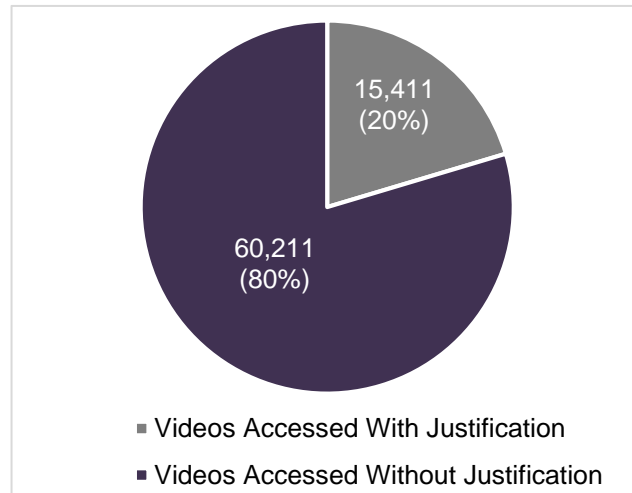
Consistent with best practices, we recommend that standard operating procedures outline a specific review process for ensuring compliance with the body-worn camera policies, including proper activation, uploading, and categorization. To enhance accountability, the policy should outline the number of videos supervisors should review, how supervisors should select videos, how frequently they should conduct reviews, and how they should document the review. We recommend that the department strengthen the policy to require supervisors to randomly review a specific number of videos each month and document their review findings.

Users Failed to Document Video Access

We found that 20% of the 75,622 videos streamed between November 2016 and May 2018 contained a reason for why the video was viewed (see Exhibit 9). When accessing body-worn camera video footage, zone supervisors, officers, and other users are required to enter notes into the videos management system to explain why they accessed the footage. Failure to comply with this procedure may violate citizens' privacy and disrupt the chain of custody, which could affect the evidentiary value of the video evidence in court proceedings. We recommend that the department enforce this policy and develop standardized justifications for users to enter into the video management system when accessing body-worn camera footage.

Users did not provide notes to explain their access to body-worn camera footage. As shown in Exhibit 9, only 20% of the 75,622 videos streamed by officers and other users between November 2016 and May 2018 included justification notes. The department's policy requires an employee or supervisor to include a note in the video management system that details the reason for accessing the footage.

Exhibit 9: Users Did Not Explain Reasons for Accessing Video Footage



Source: Data from video management system evidence created report from November 2016 to May 2018

Where a justification for accessing the video was included, it was not always clear whether the notes officers and supervisors used to justify accessing footage would have satisfied the department's expectations. We saw examples in which officers' notes included the case number or the call signal, not a specific reason for accessing the video, such as "accessed for ongoing investigation" or "accessed during training." The department has not standardized the wording of the notes that officers and supervisors should use before accessing body-worn camera video evidence.

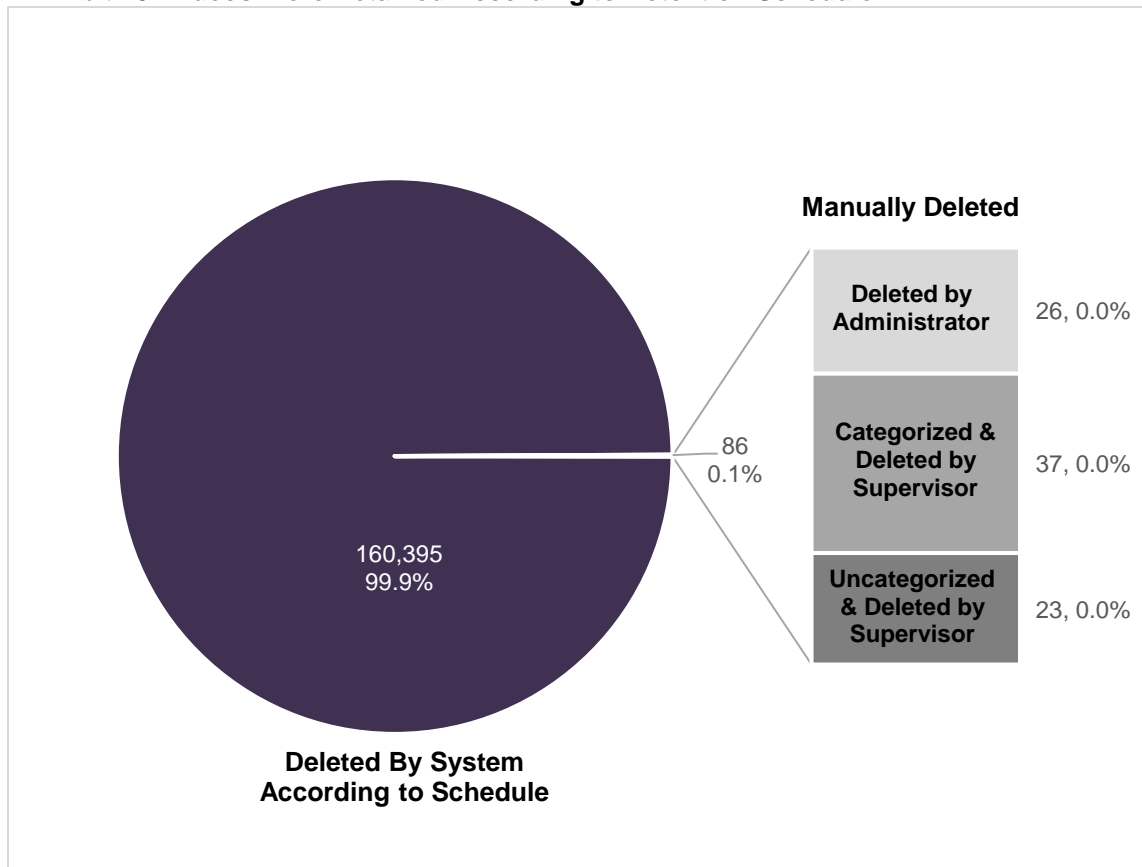
Best practices encourage police departments to protect the integrity and security of body-worn camera data by using a video management system with built-in audit trails and records of who accesses videos, when, and for what purpose, to preserve the evidence chain of custody. The department's video management system has built-in user, video, and device audit trails. Because the system functions as a digital evidence locker, officers and supervisors who access footage without proper documentation could adversely affect the chain of custody of evidentiary data. Digital evidence must be authenticated in court, similar to physical evidence, and undocumented access to it could undermine its evidentiary value.

We recommend that the department enforce the policy to provide reasons for accessing body-worn camera video footage. We also recommend that the department develop standardized justifications for users to enter into the video management system when accessing body-worn camera footage.

Video Management System Deleted Videos According to Policy, But Manual Deletions Bypassed System Controls

The video management system deleted 160,395 (99%) of 160,480 deleted videos according to the department's video retention schedule; however, we found that 86 videos were manually deleted by administrators and supervisors before the scheduled deletion date (see Exhibit 10). System controls are designed to delete videos based on categorization and according to the department's retention policy. Uncategorized videos are not automatically deleted by the system. While the department's policy does not address who is allowed to delete video footage, the department stated that the video management system is configured to prevent users without administrative access from deleting footage.

Although the video management system automatically deletes videos based on retention schedule, it maintains an audit trail of the record for future reference. As shown in Exhibit 10, system administrators deleted 26 videos before the scheduled deletion date. Officers with supervisor access manually deleted 60 videos—37 uncategorized videos and 23 categorized videos—before the retention period ended. We confirmed with the compliance team one of the supervisors was an administrator of the taser program and received temporary administrative access to delete non-evidentiary footage.

Exhibit 10: Videos Were Retained According to Retention Schedule

Source: Data from video management system evidence deleted report from November 2016 to May 2018

The compliance team told us that the system should retain uncategorized footage until an administrator manually deletes it. The compliance team is also responsible for reviewing footage scheduled for deletion to ensure that it was properly categorized. To protect against deletions related to improper categorization, administrators can recover videos up to 7 days after their retention period expires.

Best practices suggest police departments should retain body-worn camera footage long enough to demonstrate transparency to the public. Deleting evidentiary data before the scheduled retention date reduces accountability and transparency. We recommend that the department conduct monthly reviews of user roles and permissions to ensure that users have appropriate access to the video management system and to determine whether non-administrative users can delete videos. To increase accountability and transparency, compliance administrators should categorize footage before deletion. We also recommend the department

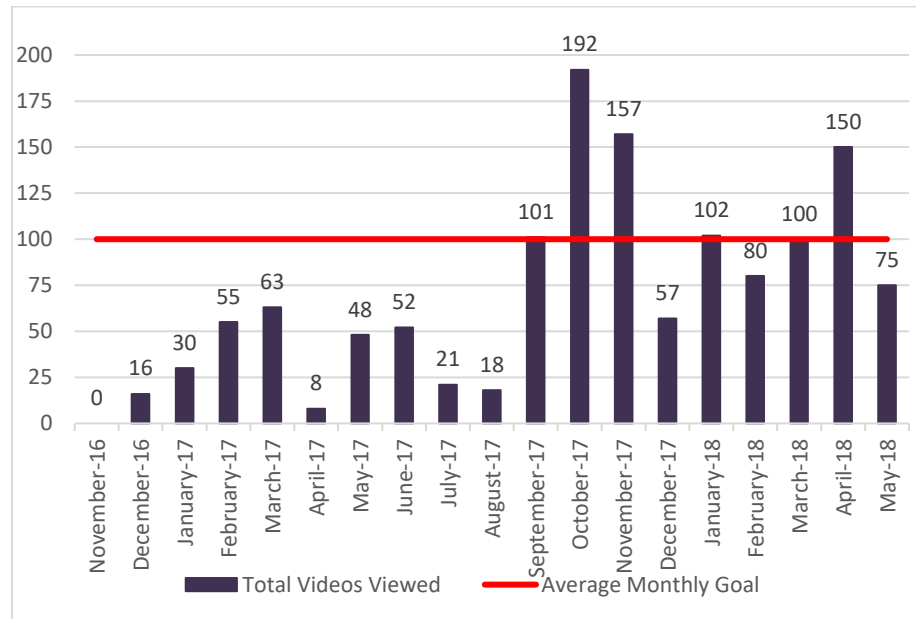
monitor and track videos that are manually deleted before the retention schedule to promote accountability.

Compliance Administrators Could Improve Training and Monitoring Efforts

The compliance team does not appear to be reviewing body-worn camera videos as required. Between November 2016 and May 2018, the compliance team streamed 1,325 videos—less than 1% of the total videos captured from November 2016 to May 2018. The compliance team is responsible for reviewing footage to track compliance with body-worn camera policy. The team is also required to review videos scheduled for deletion to assess whether any videos were miscategorized. We found that this verification occurred on only 1,543 of the 155,094 videos deleted between May 2017 and May 2018. Also, the department has not offered refresher training for officers since the body-worn camera program was first implemented in late 2016.

In December 2017, the department modified procedures to require the compliance administrator to conduct a random audit of a minimum of 25 body-worn camera videos on a weekly basis. Administrators did not consistently meet the new requirements as of May 2018 (see Exhibit 11). Since the procedural change, the compliance team has viewed at least 100 videos per month in three of the six months (January, March and April of 2018). The procedure stated the data should be analyzed and a report documenting the findings should be generated monthly. The compliance team reviews are important to ensure that officers and zone supervisors understand program requirements, to provide an opportunity for the compliance administrator to offer clarity and additional training if necessary, or to propose policy changes to ensure that officers' and zone supervisors' actions match policy requirements. Prior to December 2017, the compliance administrator was required to conduct semi-annual audits.

Exhibit 11: Administrators Do Not Review Camera Footage According to Policy



Source: Supervisor audit trails from the video management system from November 2016 through May 2018

We recommend that the compliance team review the body-worn camera footage in accordance with procedures to ensure that officers are following policies and that videos scheduled for deletion are properly categorized.

The department has not offered refresher training on body-worn camera policies since the program was first implemented in late 2016. Although the department revised its policy in December 2017, which included changing the types of calls that officers are required to record, the compliance team has not offered refresher courses. Zone 4, which the department first equipped with body-worn cameras in November 2016, has not had additional training on the body-worn cameras since the program's inception.

The compliance team offers body-worn camera training for three groups: recruits, officers, and investigators. Based on the training materials that we reviewed from the compliance team, all three trainings cover device functionality, officers' minimum duties, retention periods, and chain of custody. We noted that some supervisors appear to be unaware of standard operating procedures related to the body-worn camera program. To ensure policy compliance, we recommend that the compliance administrator hold department-wide body-worn camera refresher trainings based on the most recent policy updates.

Recommendations

To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police:

1. clarify the policy to state whether all officers responding to an incident must record body camera video
2. update the policy to remove the requirement that supervisors upload videos of use-of-force incidents and to require supervisors to review the audit trail to ensure the involved officer has not accessed the video prior to writing the report
3. clarify criteria for labeling and categorizing videos in standard operating procedures
4. establish a formal process for zone supervisors' periodic reviews, including the number and selection of videos, frequency, and required documentation
5. conduct monthly reviews of user roles and permissions to determine if non-administrator users can delete videos
6. enforce policies requiring the compliance team to review all deleted footage prior to deletion for miscategorization
7. develop standard justifications for accessed footage to ensure compliance with the policy

To ensure accountability and transparency, we recommend the chief of police monitor and track the following performance metrics:

The number and percentage of:

8. videos captured compared to the number of dispatched calls, using the 80% threshold as a comparative benchmark
9. videos uploaded to the system within one day
10. uncategorized videos
11. videos streamed by supervisors
12. videos deleted before the retention schedule
13. videos audited by the compliance team
14. audited videos that complied with activation procedures
15. audited videos that complied with deactivation procedures
16. audited videos categorized accurately

Appendix

Appendix A: Management Review and Response to Audit Recommendations

Report # 18.06	Performance Audit: Body-Worn Camera Program	Date: 11/ 2018
Recommendation 1: To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police clarify the policy to state whether all officers responding to an incident must record body camera video.		
Proposed Action: The existing SOP does not provide the level of clarity required for a large organization. The SOP will be modified to eliminate those factors causing confusion.		Response: Agree
Person Responsible: Deputy Chief L. Hagin		Implementation Date: 12/2018
Recommendation 2: To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police update the policy to remove the requirement that supervisors upload videos of use-of-force incidents and to require supervisors to review the audit trail to ensure the involved officer has not accessed the video prior to writing the report.		
Due to a more complete audit trail, the policy will be revised to remove the requirement that supervisors upload videos of use-of-force incidents. The policy will now require the immediate supervisor to review the audit trail for compliance by the involved officer with the policy not to access the video prior to completing the initial incident report.		Response: Agree
Person Responsible: Deputy Chief Lane Hagin		Implementation Date: 12/2018
Recommendation 3: To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police clarify criteria for labeling and categorizing videos in standard operating procedures.		
Proposed Action: The SOP has too many coding options, which has caused confusion and diminished performance. Initially there were 32 coding options, this has been reduced to 19, and the goal is 10 options. This reduction of choices should provide the necessary adjustments to allow for greater efficiency and consistency.		Response: Agree
Person Responsible: DC L. Hagin		Implementation Date: 12/2018

Recommendation 4:

To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police **establish a formal process for zone supervisors' periodic reviews, including the number and selection of videos, frequency, and required documentation.**

Proposed Action: Each Zone is going to be required to have their administrative sergeant audit 25 recordings every 2-weeks. They will be required to document the specific recordings examined, whether they were properly labeled, whether the officer met stated recording requirements, and whether the Zone's UAF footage corresponds to the number of UAF incidents captured in the 911 Center. The Audit Team will be responsible for managing compliance with this requirement.

Response:
Agree

Person Responsible: DC L. Hagin

Implementation Date:
01/2019

Recommendation 5:

To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police **conduct monthly reviews of user roles and permissions to determine if non-administrator users can delete videos.**

Proposed Action: The department recognizes the need to regularly update access controls in the Evidence.com platform. There are personnel that depart, and others who change roles within our agency. Those that depart must be removed from Evidence.com access, and those who change roles need to have access appropriate to their assigned position. Tracking access also allows the BWC Team to track the status of BWCs no longer assigned and enables the team to put them back into circulation. The updating of access controls within Evidence.com will occur regularly, at least monthly.

Response:
Agree

Person Responsible: N/A

Implementation Date:
12/2019

Recommendation 6:

To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police **enforce policies requiring the compliance team to review all deleted footage prior to deletion for miscategorization.**

Proposed Action: The retention period was modified, and all videos are saved for 5-years. Additionally, there are only 2 individuals with the authority to delete videos, and their accounts will be cross-checked by supervisory personnel. This policy amendment was made during the audit.

Response:
Partially Agree

Person Responsible: N/A

Implementation Date:
Complete

Recommendation 7:

To ensure compliance with the department's body-worn policies and best practices, we recommend that the chief of police **develop standard justifications for accessed footage to ensure compliance with the policy.**

Proposed Action: The requirement to provide a specific reason for viewing a video is not an essential metric. The "notes box" is only available in Evidence.com after the video is uploaded, you are unable to add notes as to why you viewed a video in the Axon View App or in Axon Sync on the MDT, so it is not trackable across the range of viewing options.

We are requiring that administrative sergeants and supervisors review BWC video to ensure the BWCs are activated and deactivated in accordance with policy, and not interrupted during recording. The supervisors will also audit to ensure the BWC is used according to policy. Only the officer assigned the BWC, his immediate supervisor(s), and the administrative sergeant can access the individual officer's BWC in Evidence.com. The requirement to label why a video is accessed only in Evidence.com, and not in the other viewing options makes this metric impossible to accurately track and enforce. The SOP will be amended accordingly.

Response:

Agree

Person Responsible: N/A

Implementation Date:

01/2019

Recommendations 8-16:

To ensure accountability and transparency, we recommend the chief of police monitor and track the following performance metrics **for the number and percentage of:**

8. **videos captured compared to the number of dispatched calls, using the 80% threshold as a comparative benchmark**
9. **videos uploaded to the system within one day**
10. **uncategorized videos**
11. **videos streamed by supervisors**
12. **videos deleted before the retention schedule**
13. **videos audited by the compliance team**
14. **audited videos that complied with activation procedures**
15. **audited videos that complied with deactivation procedures**
16. **audited videos categorized accurately**

Proposed Action: Metrics must be developed that allow for improved performance. The Zone audits will encompass much of the above-referenced, while a final audit checklist is still being identified.

Response:

Agree

Person Responsible: DC L. Hagin

Implementation Date:

01/2019